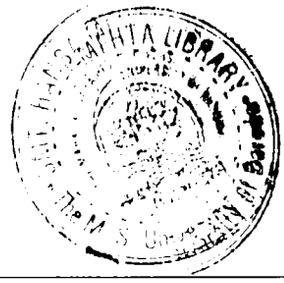

CHAPTER - 1

Indian Banking: Milestone & a road ahead

- ☑ Introduction
- ☑ Pre-Independence Banking Scenario in India
- ☑ Post-Independence Developments in Banking Sector
- ☑ Banking Sector Reforms since 1991
- ☑ Current Issues in Indian Banking
- ☑ Future of India's Banking Sector
- ☑ Concept of E-banking
- ☑ E-banking and RBI
- ☑ E-banking Challenges and Concerns
- ☑ E-banking: Risks and Their Management

CHAPTER: 1

INDIAN BANKING: MILESTONE & A ROAD AHEAD

Introduction:

With the Indian economy moving on to a high growth trajectory, consumption levels soaring and investment riding high, the Indian banking sector is at a watershed. Further, as Indian companies globalize and people of Indian origin increase their investment in India, several Indian banks are pursuing global strategies. The industry has been growing faster than the real economy, resulting in the ratio of assets of commercial banks to GDP increasing to 92.5 per cent at end-March 2007[1]. The Indian banks have also been doing exceptionally well in the financial sector with the price-to-book value being second only to china, according to a report by Boston Consultancy Group.

1.1 Pre-Independence Banking Scenario in India [2]:

In India, the ancient Hindu Scriptures refer to the money lending activities in the Vedic period. During the Ramayana and Mahabharata eras, banking had become full-fledged business activity and during the Manu Smriti period which followed the Vedic period and Epic age, the business of banking was carried on by the members of the Vaish Community. Banking is different from money lending but two terms have in practice been taken to convey the same meaning. Banking has two important functions to perform, one of accepting deposits and other of lending money or investment of funds. During the Moguls period, metallic money was issued and the indigenous bankers added one more line of money changing to their already profitable business. They started exchanging money circulating in one part of the country with the money current in another part of the country making good margin for them.

The English traders, who came to India in the 17th century, established some contracts with the indigenous bankers by borrowing funds from them in 1786. The English Agency House had established the Bank of Bengal at Calcutta with the advent of modern banking conducted on western lines, the indigenous bankers lost further importance.

The English House Agency in Calcutta and Bombay were the bankers to the East India Company and the European merchants in India. They had no capital of their own and depend mainly on deposits from the public for finance. These agency houses failed as they combined banking with trading. Among the earliest banks in established in India, were the Bank of Bengal (1806), Bank of Bombay (1840) and Bank of Madras (1843).

These banks were also known as "presidency banks". In 1860 the concept of limited liability was introduced in banking. These banks (presidency banks) were allowed to issue notes to a limited extent, but this right was taken over by the government in 1862. In view of limited liability, several joint stock banks were floated. Some of important banks were established during 1860 to 1900, were:

Table - 1.1: List of Banks established during 1860 - 1900

Sr. No	Bank Name
1	Allahabad Bank Ltd.
2	The Alliance bank of Simla Ltd.
3	The Oudh Bank Ltd.
4	The Púnjab national Bank Ltd.

[Source: RBI Report on trend & progress on Banking in India, Several Issues]

Thus by the end of year 1900, there were three classes of banks in India

Table 1.2: Different Classes of Banks in India at the end of year 1900.

Sr. No	Bank Name
1	Presidency Banks, numbering 3
2	Joint Stock Banks, numbering 9
3	Exchange Banks or Foreign Banks, numbering.

[Source: RBI Report on trend & progress on Banking in India, Several Issues]

The swadeshi movement which started in the early 1900s gave stimulus to the growth of indigenous joint Stock Banks. Some of the banks established during the 1900 to 1910 period were,

Table 1.3: List of Banks established during the period of 1900 - 1910

Sr. No	Bank Name
1	The Peoples Bank of India Ltd.
2	The Bank of India Ltd.
3	The Bank of Baroda Ltd.
4	The Central Bank of India Ltd.

[Source: RBI Report on trend & progress on Banking in India, Several Issues]

In 1921, the 3 presidency banks were merged to form the Imperial Bank of India. During 1900 and 1950, the Indian joint stock banks specialized in providing short term credit, for trade in the form of cash-credit and over draft facilities, foreign exchange business, remained the monopoly of foreign banks. Between 1900 and 1925 many banks failed due to various reasons. The Central Banking Enquiry Committee was constituted in 1929; it gave the reasons for the failure of banks such as: refer table 1.4.

On the basis of major recommendations of the central Banking Enquiry Committee the RBI Act was passed in 1934. While in 1949 the Banking Regulation Act was passed for regulation and supervision of banks.

Table 1.4: Various reason for failure of banks during 1900 - 1925

Sr. No.	Particular
1	Insufficient capital.
2	Poor liquidity of assets.
3	Combination of non-banking activities with banking activities.
4	Irrational credit policy.
5	Incompetent and inexperienced directors.

[Source: RBI Report on trend & progress on Banking in India, Several Issues]

It gave wide power to RBI to regulate, supervise and develop the banking systems. During 1950 to 1969 two important developments took place, first, the all India Rural Credit Survey Committee, which examined the issue of credit availability at the rural areas, recommended the creation or a state partnered sponsored bank entrusted with the task of opening branches in the rural areas.

Accepting this recommendation, the State Bank of India Act was passed in 1955 and the Imperial Bank of India was renamed as State Bank of India. Later in 1959 the State Bank of India (Subsidiary Bank) Act was passed enabling SBI, to take over 8 princely state associated banks as the subsidiaries; these banks were,

Table 1.5: List of Subsidiaries bank of SBI in 1959

Sr. No.	Bank
1	State Bank of Bikaner
2	State Bank of Hyderabad
3	State Bank of Indore
4	State Bank of Jaipur
5	State Bank of Mysore
6	State Bank of Patiala
7	State Bank of Saurashtra
8	State Bank of Travancore

[Source: RBI Report on trend & progress on Banking in India, Several Issues]

Secondly the need about wider diffusion of banking facilities and to change the uneven distributive pattern of bank lending was realized. The scheme of social control over banks was announced in the parliament in December 1967. The National Credit Control Council was set up in 1968 to assess the demand for bank credit from various sector of the economy and to determine their respective priorities in allocation.

1.2 Post-Independence Developments in Banking Sector [3]:

On the eve of independence in August 1947, there were 648 commercial banks, comprising 97 scheduled and 551 non scheduled banks. Development in banking sector is divided into two separate groups namely pre-nationalize period and post nationalize period:

1.2.1 Pre-Nationalization Period:

The year 1969 was a landmark in the history of commercial banking in India. In July of that year, the government nationalized 14 major commercial banks of the country. In April 1980, government nationalized 6 more commercial banks.

In 1951, when the First Five Year Plan (1951 - 56) was launched, the development of rural India was accorded the highest priority. The All India Rural Credit Survey Committee recommended. the creation of a State - partnered and State, sponsored bank by taking over the Imperial Bank of India and integrating with it, the former State - owned or State - associated banks. Accordingly, an Act was passed in the Parliament in May 1955 and the. State Bank of India was constituted on July 1, 1955.

Later, the State Bank of India (Subsidiary Banks) Act was passed in 1959 enabling the State Bank of India to take over eight former States - associated banks as its subsidiaries. During the pre-nationalization period, the industrial sector claimed the lion's share in bank credit. Within the industry, the large - scale sector cornered the bulk of credit and the share of small - scale industries was marginal. There were many reasons for the dominance of large industrial companies in the banking sector.

A disturbing feature of the pre-nationalization banking policy was the negligible share of agricultural sector in bank credit. This share hovered around 2 per cent of total commercial bank credit. The privately owned commercial banks were neither interested nor geared to meet the risky and small credit requirements of the farmers. Similarly, the share of other non-industrial sectors in bank credit was also low. Since the commercial banks were under the control of big industrialists, the lendable funds of the banks were sometimes used to finance socially undesirable activities like hoarding of essential commodities.

1.2.2 Post Nationalization Period [4]:

As already noted, leading commercial banks of the country were nationalized in1969 with the following objectives in view:

- ❖ To break the ownership and control of banks by a few business families.
- ❖ To prevent concentration of wealth and economic power.
- ❖ To mobilize savings of the masses from every nook and corner of the country.
- ❖ To pay greater attention to the credit needs of the priority sectors like agriculture and small industries.

The post nationalization period witnessed a remarkable expansion in the banking and financial system. The biggest achievement of nationalization was the reallocation of sectoral credit in favour of agriculture, small industries and exports which formed the core of the priority sector. Within agriculture, credit for the procurement of food grains (food credit) was a major item. Other agricultural activities preferred for credit included poultry farming, dairy and piggeries. Certain other sectors of the economy which also received attention for credit allocation were: professionals and self employed persons, artisans and weaker sections of society. Conversely, there was a sharp fall in bank credit to large scale industries. However, the share of small scale industry registered an upward trend.

Nationalization of commercial banks was a mixed blessing: After nationalization there was a shift of emphasis from industry to agriculture. The country witnessed rapid expansion in bank branches, even in rural areas. Branch expansion programme led to mobilization of savings from all parts of the country. Nationalized banks were able to pay attention to the credit needs of weaker sections, artisans and self – employed. However, bank nationalization created its own problems like excessive bureaucratization, red tapism and disruptive tactics of trade unions of bank employees.

1.3 Banking Sector Reforms since 1991[5]:

Until the early 1990s, the banking sector suffered from lack of competition, low capital base, low productivity and high intermediation cost. Commenting on the performance of the nationalized banks, the Reserve Bank of India observed, "After the nationalization of large banks in 1969 and 1980, the Government owned banks have dominated the banking sector. The role of technology was minimal and the quality of service was not given adequate importance. Banks also did not fallow proper risk management systems and the prudential standards were weak. All these resulted in poor asset quality and low profitability." Prior to reforms, the Indian Government determined the quantum, allocation and the price of credit, a situation referred to as financial repression by some experts. It was in this backdrop, that wide - ranging banking sector reforms in India were introduced as an integral part of the economic reforms initiated in the early 1990s. Reforms in the commercial banking sector had two distinct phases.

1.3.1 The First Phase:

The first phase of reforms implemented subsequent to the release of the Report .of the Committee on Financial System (Chairman: M. Narasimham), 1992 (or Narasimham Committee I) focused mainly on enabling strengthening measures. The Committee was guided by the fundamental assumption that the resources of the banks come from the general public and held by the banks in trust. These resources have to be deployed for maximum benefit of their owners, i.e., the depositors. This assumption automatically implies that even the Government has no business to endanger the solvency, health and efficiency of the nationalized banks. According to the Committee, the poor financial shape and low efficiency of public sector banks was due to: (a) extensive degree of central direction of their operations, particularly in terms of investment, credit allocation and branch expansion and (b) excessive political interference, resulting into failure of commercial banks to operate on the basis of their commercial judgment and in the

framework of internal economy. Despite opposition from trade unions and some political parties, the Government accepted all the major recommendations of the Committee some of which have already been implemented.

1.3.2 The Second Phase:

The second phase of reforms, implemented subsequent to the recommendations of the Committee on Banking Sector Reforms (Chairman : M. Narasimham), 1998 (or Narasimham Committee II) placed greater emphasis on structural measures and improvement in standards of disclosure and levels of transparency in order to align the Indian standards with international best practices.

1.3.3 Objectives of Banking Sector Reforms[6]:

The key objective of reforms in the banking sector in India has been to enhance the stability and efficiency of banks. To achieve this objective, various reform measures were initiated that could be categorized broadly into three main groups:

- Enabling measures.
- Strengthening measures and
- Institutional measures.

Enabling measures were designed to create an environment where banks could respond optimally to market signals on the basis of commercial considerations. Salient among these included reduction in statutory pre-emotions so as to release greater funds for commercial lending, interest rate deregulation to enable price discovery, granting of operational autonomy to banks and liberalization of the entry norms for financial intermediaries. The strengthening measures aimed at reducing the vulnerability of banks in the face of fluctuations in the economic environment. These included, inter alia, capital adequacy, income recognition, asset classification and provisioning norms, exposure norms, improved levels of transparency, and disclosure standards. Institutional framework conducive to development of banks

needs to be developed. Salient among these include reforms in the legal framework pertaining to banks and creation of new institutions.

1.3.4 Contents of Banking Sector Reforms [7]:

Banking sector reforms since 1991 have included, among others, the following:

- Granting operational autonomy to banks.
- Liberalization of entry norms for banks.
- Reduction in statutory pre - emption so as to release greater funds for commercial lending.
- Deregulation of interest rates.
- Relaxation in investment norms for banks.
- Easing of restrictions in respect of banks foreign currency investments.
- Withdrawal of reserve requirements on inter - bank borrowings.

Thus, financial repression has eased substantially with the deregulation of interest rates and substantial removal of credit allocation.

Cash Reserve Ratio (CRR):

Scheduled banks in India are required statutorily to hold cash reserves, called cash reserve ratio (CRR), with the RBI. Increase / decrease in CRR is used by the RBI as an instrument of monetary control, particularly to mop up excess increases in the supply of money. This power was given to RBI in 1956.

Narasimham Committee I recommended that RBI should rely on open market operations increasingly and reduce its dependence on CRR. This would reduce the amount of cash balances of the banks with the RBI enabling them to increase their revenues through more investments. It proposed that CRR should be progressively reduced from the then existing level of 15 per cent to 3 to 5 per cent.

CRR was gradually lowered from its peak at 15 per cent during July 1989 to April 1993 to 8.0 per cent in April 2000. It stood at 5 per cent effective October 2, 2004. In this connection, the Ninth Five Year Plan (1997 - 2002) remarked, "the level of the cash reserve ratio (CRR) that is to be maintained by the Indian banks is considerably higher than the international levels which are specified for prudential reasons. Although in recent years there has been significant reduction in the CRR from 15 per cent to 10 per cent and also the interest paid on CRR deposits with the RBI has been raised from 3.5 per cent to 4.5 per cent, there is a view that the CRR should be reduced even further, preferably to 3 per cent."

Statutory Liquidity Ratio (SLR):

Apart from the CRR, banks in India are also subject to statutory liquidity requirement; Under this requirement, commercial banks along with other financial institutions like Life Insurance Corporation of India (LIC), the General Insurance Corporation (GIC) and the Provident Funds are required under law to invest prescribed minimum Proportions of their total assets / liabilities in government securities and other approved securities. The underlying philosophy of this provision is to allocate total bank credit between the government and the rest of the economy. The assurance of a certain minimum share of bank credit to the government affects the borrowings of the government from the RBI and hence serves as a tool of quantitative monetary control. The SLR provision has created a captive market for government securities which increases automatically with the growth in the liabilities of the banks. Moreover, it has kept the cost of the debt to the government low in view of the generally low rate of interest on government securities.

Narasimham Committee I asked the Government to reduce the SLR from the then existing 38.5 per cent to 25 percent over a period of five years. A reduction in the SLR levels would leave more funds with the banks which could allocate them to

promote agriculture, industry and trade. The Committee further recommended that Government borrowing rates should be progressively market related so that higher rates would help banks to increase their income from their SLR investments. SLR was reduced from its peak of 38.5 per cent during September 1990 to 25 per cent in October 1997.

Structure of Interest Rates:

Narasimham Committee I recommended that the level and structure of interest rates in the country should be broadly determined by market forces. All controls and regulations on interest rates on lending should be removed. The country has moved towards liberalized credit allocation mechanism and reduced direct control over interest rates by the monetary authorities. Interest rate slabs have been gradually reduced from 20 to 3. Similarly, interest rates have been deregulated on the high slabs of bank rates. The purpose of deregulation is to promote healthy competition among the banks and encourage their operational efficiency. Scheduled banks have now the freedom to set interest rates on their deposits subject to minimum floor rate (4.5 per cent) and maximum ceiling rate (11 per cent).

Prime lending rates of banks for commercial credit are now entirely within the purview of the banks and are not set by the RBI. The domestic interest rates which are still subject to regulation are the rate of interest on saving accounts and rates of interest on export credit. In line with the decline in inflation rate and also in view of the importance of lower real interest rates in accelerating industrial growth and boosting India's competitiveness abroad, RBI reduced the Bank Rate (3) from 8 per cent to 7 per cent, effective April 2, 2000. Rate of interest on saving deposits of commercial banks was also reduced from 4.5 per cent to 4.0 per cent. Following these measures, the structure of interest rates in India has come closer to ruling international rates.

Organization of Banking Structure:

Narasimham Committee I proposed a substantial reduction in the number of public sector banks through mergers and acquisitions. The broad pattern should consist of:

- 3 or 4 large banks which could become international in character.
- 8 or 10 national banks with a network of branches throughout the country.
- Local banks whose operations would be generally confined to a specific region.
- Rural banks whose operations will be confined to rural areas.

Significantly, Narasimham Committee I recommended that RBI should permit the setting up of new banks in the private sector. It wanted a positive declaration from the Government that there would be no more nationalization of banks. It further recommended that there should not be any difference in treatment between the public sector banks and the private sector banks.

It recommended that RBI should follow a more liberal policy in respect of all owing the foreign banks to open branches in India and they should be subjected to the same requirements as are applicable to the Indian banks.

In January 1993, RBI had issued guidelines for licensing of new banks in the private sector. It had granted licenses to 10 banks which are presently in business. Based on a review of experience gained on the functioning of new private sector banks, revised guidelines were issued in January 2000. Following are the major revised provisions:

- Initial minimum paid-up capital shall be Rs. 200 crore which will be raised to Rs.300 crore within three years of commencement of business.

- Contribution of promoters shall be a minimum of 40 per cent of the paid up capital of the bank at any point of time. This contribution of 40 per cent shall be locked in for five years from the date of licensing of the bank.
- While augmenting capital to Rs. 300 crore within three years, promoters shall bring in at least 40 per cent of the fresh capital which will also be locked in for five years.
- NRI participation in the primary equity of a new bank shall be to the maximum extent of 40 per cent.

Duality of Control:

Narasimham Committee I recommended removal of duality of control over the banking system by the banking department of the Finance Ministry on the one hand, and by the RBI on the other hand. The Committee desired the RBI to assume full responsibility of overseeing the functioning of the banking system.

Abolition of Selective Credit Controls (SCCs):

SCCs, introduced in India in 1956, pertain to regulation of credit for specific purposes. The techniques of SCCs used by the RBI include fixing minimum margins for lending against securities, ceiling on maximum advances to individual borrowers against stocks of certain commodities, and minimum discriminatory rates of interest prescribed for certain kinds of advances. SCCs have been used mainly to prevent the speculative holding of essential commodities like food grains to prevent price rise. Selective credit controls have been abolished in the post liberalization period.

Other Measures:

Credit restrictions for purchase of consumer durables have been removed / relaxed. Similarly, coverage of priority sector has been enlarged by the inclusion of software, agro - processing, industries and venture capital. These measures have given the banks the much - needed flexibility to manage their asset portfolios.

Commenting on the success of banking sector reforms, the Reserve Bank of India observed, "There is evidence to suggest that competition in the banking industry has intensified. Significant improvement was 1ilso discernible in the various parameters of efficiency, especial intermediation costs, which declined significantly. Profitability of commercial banks, on the whole, improved significantly despite a decline in spread and higher provisioning following the introduction and subsequent tightening of prudential norms."

1.4 Current Issues in Indian Banking [8]:

Despite substantial improvements in the banking sector, some issues have to be addressed over time as the reform process is entrenched further. The discussion on banking developments revolves around on a wide range of issues like:

- Overall redrawing of boundaries between the State ownership of financial entities and private sector ones.
- Public sector character of the banking sector and efficiency.
- Dilution of the government stake and its impact on the performance of the banking sector.
- Corporate governance in banks and other segments of the financial system.
- Transparency of policies and practices of monetary and financial agencies and accountability.
- Prudential requirements of market participants together with comprehensive and efficient oversight of the financial system.
- Maintenance of best practices in accounting and auditing, as also collection, processing and dissemination of symmetric and detailed information to meet the market needs.
- Relevance of Development Finance Institutions (DFIs).

The commonality among these concerns has given rise to a wide recognition and acceptance of having a set of international standards and best practices that every systemically important country should strive to foster and implement. Financial sector reforms, introduced in the early 1990s in a gradual and sequenced manner, were directed at the removal of various deficiencies from which the system was suffering. The basic objectives of reforms were to make the system more stable and efficient so that it could contribute in accelerating the growth process.

In response to reforms, the Indian banking sector has undergone radical transformation during the 1990s. Reforms have altered the organizational structure, ownership pattern and domain of operations of institutions and infused competition in the financial sector. The competition has forced the institutions to reposition themselves in order to survive and grow. The extensive progress in technology has enabled markets to graduate from outdated systems to modem market design, thus, bringing about a significant reduction in the speed of execution of trades and transaction costs.

With the increasing integration of various segments of financial markets, the distinctions between banks and other financial intermediaries are also getting increasingly blurred. Another important aspect of reforms in the financial sector has been the increased participation of financial institutions, especially banks, in the capital market. These factors have led to increased inter - linkages across financial institutions and markets. While increased inter - linkages are expected to lead to increased efficiency in the resource allocation process and the effectiveness of monetary policy, they also increase the risk of contagion from one segment to another with implications for overall financial stability. This would call for appropriate policy responses during times of crisis. Increased inter - linkages also raise the issue of appropriate supervisory framework.

Banking sector reforms in India are grounded in the belief that competitive efficiency in the real sectors of the economy will pot realize its full potential unless the banking sector was reformed as well. Thus, the principal objective of banking sector reforms was to improve the allocative efficiency of resources and accelerate the growth process of the real sector by removing structural deficiencies affecting the performance of banks.

In India, while the banking system continues to play a predominant role, it is significant to note that, as a result of various reform measures, the relative significance of financial markets has increased. This augurs well for the overall stability of the financial system. The East Asian crisis has also underlined the need for a balanced financial system wherein financial markets also play an important role in providing necessary liquidity, especially during times of crisis. Banking system also requires liquidity in times of stress, which only deep and liquid financial markets can provide.

1.5 Future of India's Banking Sector [9]:

Banking sector reforms in India are by no means complete. Plans are afoot to modernize the financial system to make it compatible with best international practices.

1.5.1 Vision Document for Payment Systems: 2005 – 08[10]:

In the recent period, the RBI has taken a number of initiatives to strengthen the institutional, technological and procedural framework for the payment and settlement systems. To carry forward these initiatives in an integrated and cohesive manner, a Vision Document for 2005 – 08 has been prepared after taking into consideration the feedback from the various stakeholders such as banks, technology solution providers, members of public and other experts in the field.

The Vision Document sets out the roadmap for implementing the vision for payment and settlement systems within the next three years. The key themes of the action plans identified in the Vision Document are safety, security, soundness and efficiency (Triple-S and E). While safety in payment and settlement systems relates to risk reduction measures, security implies confidence in the integrity of the payment systems. All payment systems are envisaged to be on a sound footing with adequate legal backing for operational procedures and transparency norms. Efficiency enhancements are envisaged by leveraging the benefits of technology for cost effective solutions.

The main action points for payment and settlement systems, 2005 - 08 as set out in the Vision Document are indicated below:

Action Points during 2005 - 06:

- Pursuing with Indian Banks Association and major banks for setting up of a national level entity which will operate all retail payment systems in the country;
- Operationalizing National Settlement System for all clearings at four metro centers by December 2005;
- Finalizing the proposed Electronic Funds Transfer (EFT) regulations;
- Implementing Stage-2 of RTGS System, i.e., Integrated Accounting System (IAS) - RTGS rollout during which all inter - bank transactions at all major centers would be settled on RTGS platform and paper - based inter - bank clearing will be closed;
- Pursuing with RTGS participants to cover all their networked branches under RTGS framework paving way for RTGS based customer related transactions at about ten thousand branches in the country;
- Implementing image - based Cheque Truncation System (CTS) at the National Capital Region (NCR) on a pilot basis;

- ❖ Preparing minimum standard of operational efficiency at MICR Cheque Processing Centre (CPC);
- ❖ Making available EFT facility at 500 capital market intensive centers as identified by BSE and NSE;
- ❖ Setting up Customer Facilitation Centre (CFC) at the RBI for various segments of national payment systems;
- ❖ Public disclosure from each payment service provider of its standards, terms and conditions under which the payment will be effected and also compensation policy and procedure for any deficiency in services including the setting up of CFC;
- ❖ Drafting the Red Book on Payment Systems in India; and
- ❖ Drafting a comprehensive legislation on payment system.

Action Points during 2006 - 07:

It is envisaged to:

- ❖ Complete the tasks initiated during 2005 - 06;
- ❖ Extend MICR clearing to 20 additional identified centres; ensure that every cheque issued follows MICR format and standards;
- ❖ Implement EFT systems at a national level through the new retail payment institution;
- ❖ Make all payment systems in India compliant with the Core Principles for Systemically Important Payment Systems (SIPS);
- ❖ Increase the reach of payment services by means of tie up and collaboration with other large coverage entities such as the post offices; and
- ❖ Facilitate government payments and receipts through electronic mode.

Action Points during 2007 - 08:

- ❖ Creating off city back up arrangements for large value national payment systems such as RTGS and G-Sec Clearing;
- ❖ Making fully functional the new organization for retail payment systems with all such payment under its umbrella; Regulating various payment systems;
- ❖ Ensuring cheque truncation based clearing at Mumbai, Chennai and Kolkata; and
- ❖ Covering National Settlement System at all major clearing houses / clearing organizations in the country.

1.5.2 Financial Sector Technology Vision Document [11]:

The RBI released the draft Financial Sector Technology Vision document on May 6, 2005. It provides a broad overview of the thrust areas of the direction provided by the RBI in respect of IT for the financial sector for more than two decades and sets out a roadmap for 2005 - 08. The Vision document focuses on

- ❖ IT for regulation and supervision,
- ❖ IT for the Financial Sector and
- ❖ IT for Government related functions.

The Vision Document envisages emerging challenges in the form of implementation of standardization across a variety of hybrid systems at different financial entities, need for decision support systems and the technology to facilitate risk based off - site supervision. It envisions common inter operable web based structures for transmission of data relating to regulatory functions and the use of a single centralized database for all information, apart from hiving off the operation of non-critical functions by the RBI. The Vision Document also visualizes Institute for Development and Research in Banking Technology (IDRBT) which is to be a premier research institute, concentrating on research and development for the

banking and financial sector, providing educational / training facilities and hiving off business related activities.

Recognizing the requirements of IT for the financial sector, the Vision Document elucidates the thrust areas of the RBI by providing generic information on various standards and approaches, IS Audit and requisite focus on business continuity plans. The Vision Document proposes that specific attention would be devoted to percolation of technology efforts to all types of banks and all sections of the customers in the banks with specific reference to the rural areas and the use of affordable technology products which can be easily used by the target clientele with inter - shareable resources.

The document also details the use of IT in the Government sector transactions (which has the largest potential to grow significantly in the years to come), with specific attention on the need for business process re-engineering, changes in rules and procedures for aligning them with e-governance in a manner so as to achieve implementable objectives.

1.5.3 Road Map for Foreign Banks in India [12]:

At present, foreign banks may operate in India through only one of the three channels, viz.

- Branches;
- A wholly owned subsidiary (WOS); or
- A subsidiary with an aggregate foreign investment up to a maximum of 74 per cent in a private bank.

With a view to delineate the direction and pace of reform process in this area and to operationalize the extant guidelines of March 4, 2004 in a phased manner, the RBI, on February 28, 2005, released the road map for presence of foreign banks in India. The roadmap is divided into two phases.

First Phase: March 2005 to March 2009:

During the first phase, between March 2005 and March 2009, foreign banks wishing to establish presence in India for the first time could either choose to operate through branches or set up a 100 per cent was, following the one mode presence criterion. For new and existing foreign banks, it is proposed to go beyond the existing WTO commitment of 12 branches in a year. Foreign banks already operating in India would be permitted to establish presence by way of setting up a WOS or conversion of the existing branches into a WOS. For this purpose, criteria such as ownership pattern, financial soundness, supervisory rating and the international ranking would be considered.

The WOS should have a minimum capital of Rs. 300 crore and would need to ensure sound corporate governance. The was will be treated on par with the existing branches of foreign banks for branch expansion with flexibility to go beyond the existing WTO commitments and preference for branch expansion in under - banked areas. The RBI may also prescribe market access and national treatment limitation consistent with WTO as also other appropriate limitations to the operations of was, consistent with international practices and the country's requirements.

During this phase, permission for acquisition of shareholding in Indian private sector banks by eligible foreign banks will be limited to banks identified by the RBI for restructuring. The RBI may, if it is satisfied that such investment by the foreign bank concerned will be in the long - term interest of all the stakeholders in the investee bank, permit such acquisition. Where such acquisition is by a foreign bank having presence in India, a maximum period of six months would be given for conforming to the "one form of presence" concept.

Second Phase: April 2009 onward:

The second phase will commence in April 2009 after a review of the experience gained and after due consultation with all the stakeholders in the banking sector. In this phase, three interconnected issues would be taken up.

First, the removal of limitations on the operations of the WOS and treating them on par with domestic banks to the extent appropriate would be designed and implemented.

Second, the WOS of foreign banks, on completion of a minimum prescribed period of operation, maybe allowed to list and dilute their stake so that, consistent with March 5, 2004 guidelines, at least 26 per cent of the paid-up capital of the subsidiary is held by resident Indians at all times. The dilution may be either by way of initial public offer or as an offer for sale.

Third, during this phase, foreign banks may be permitted to enter into merger and acquisition transactions with any private sector bank in India subject to the overall investment limit of 74 per cent.

1.6: Concept of E-banking? [13]

Electronic banking (E-banking) is a generic term encompassing internet banking, telephone banking, mobile banking etc. In other words, it is a process of delivery of banking services and products through electronic channels such as telephone, internet, cell phone etc. The concept and scope of E-banking is still evolving.

Several initiatives taken by the Government of India as well as the Reserve Bank of India (RBI) have facilitated the development of E-banking in India. As a regulator and supervisor, the RBI has made considerable progress in consolidating the existing payment and settlement systems, and in upgrading technology with a view

to establishing an efficient, integrated and secure system functioning in a real - time environment, which has further helped the development of E-banking in India. The Government of India enacted the IT Act, 2000 with effect from October 17, 2000, which provides legal recognition to electronic transactions and other means of electronic commerce.

1.6.1 E-banking: Global Experiences: [14]

Finland was the first country in the world to have taken a lead in E-banking. The Scandinavian countries have the largest number of Internet users, with up to one - third of bank customers in Finland and Sweden taking advantage of E-banking. Internet banking is also widespread in Austria, Korea, Singapore, Spain, Switzerland, etc. E-banking facilitates an effective payment and accounting system thereby enhancing the speed of delivery of banking services considerably. While the E-banking has improved efficiency and convenience, it has also posed several challenges to the regulators and supervisors.

In response to the challenges thrown by the Internet banking, regulators and supervisors from various countries have prepared their own mechanism of regulation. There is a matrix of legislation and regulations within the United States that specifically codifies the use of and rights associated with the internet and e-commerce, in general, and electronic banking and internet banking activities, in particular. The concerns of the Federal Reserve are limited to ensuring that Internet banking and other electronic banking services are implemented with proper attention to security, safety and soundness of the bank, and the protection of the banks customers.

In the UK, there is no specific legislation for regulating E-banking activities. The FSA is neutral on regulations of electronic banking. In Sweden, no formal guidance has been given to examiners by the Sveriges Bank on E-banking. General guidelines

apply equally to Internet banking activities. The role of the Bank of Finland has been, as part of general oversight of financial markets in Finland, mainly to monitor the ongoing development of Internet banking without active participation. The Reserve Bank of New Zealand applies the same approach to the regulation of both Internet banking activities and traditional banking activities. There are however, banking regulations that apply only to Internet banking. Supervision is based on public disclosure of information rather than application of detailed prudential rules.

The Monetary Authority of Singapore (MAS) subjects Internet banking to the same prudential standards as traditional banking. The MAS drafted an "Internet Banking Technology Risk Management Guidelines" in September 2002, which calls upon all banks providing internet banking to establish a sound and robust risk management process. The Hong Kong regulatory approach towards E-banking is less specific in nature. The Hong Kong Monetary Authority (HKMA) expects their banks to undertake a rigorous analysis of the security aspects of their system by getting it reviewed by qualified independent experts.

Like many of these countries, India does not have specific regulatory laws for E-banking. The existing regulatory framework over banks has been extended to Internet banking as well. However, certain guidelines have been issued to banks to recognize the risks arising from electronic modes and to devise control mechanisms that are needed to mitigate such risks. Banks offering the E-banking services in India comply with these guidelines.

1.7. E-banking and RBI: [15]

The RBI has been gearing up to upgrading itself as a regulator and supervisor of the technologically dominated financial system. In 1998, it availed the technical assistance project of Department for International Development (DFID), UK for upgrading, its supervisory system and adaptation of its supervisory functions to the

computerized environment. It issued guidelines on "risks and control in computer and telecommunication system" in February 1998 to all the banks advising them to evaluate the risks inherent in the systems and put in place adequate control mechanisms to address these risks, which can be broadly put under three heads, viz., IT environment risks, IT operations risks and product risks.

The existing regulatory framework over banks has also been extended to internet banking. These guidelines cover various issues that would fall within the framework of technology, security standards and legal and regulatory issues. Virtual banks, which have no offices and function only on line are not permitted to offer E-banking services in India and that only banks licensed under the Banking Regulation Act and having a physical presence in India are allowed to offer such services.

Further, banks are required to report to the RBI every breach or failure of security systems and procedures in Internet banking, while the RBI at its discretion may decide to commission special audit / inspection of such banks. As per recent guidelines, banks no longer need any prior approval of the Reserve Bank for offering the internet banking services. Nevertheless, banks must have their internet policy and they need to ensure that it is in line with parameters as set by the Working Group on Internet Banking in India (2001). Main recommendations of the Working Group are set forth below.

1.7.1 Main Recommendations of the Working Group on Internet Banking (Chairman: S. R. Mittal), 2001: [16]

Reserve Bank of India constituted a Working Group to examine different issues relating to internet banking and recommend technology, security, legal standards and operational standards keeping in view the international best practices. The

Group was headed by the Chief General Manager in-Charge of the Department of Information Technology and comprised experts from the fields of banking regulation and supervision, commercial banking, law and technology. The Bank also constituted an Operational Group under its Executive Director comprising officers from different disciplines in the bank, who would guide implementation of the recommendations.

The Working Group, as its terms of reference, was to examine different aspects of Internet banking from regulatory and supervisory perspective and recommend appropriate standards for adoption in India, particularly with reference to the following:

1. Risks to the organization and banking system, associated with Internet banking and methods of adopting International best practices for managing such risks.
2. Identifying gaps in supervisory and legal framework with reference to the existing banking and financial regulations, IT regulations, tax laws, depositor protection, consumer protection, criminal laws, money laundering and other cross border issues and suggesting improvements in them.
3. Identifying international best practices on operational and internal control issues, and suggesting suitable ways for adopting the same in India.
4. Recommending minimum technology and security standards, in conformity with international standards and addressing issues like system vulnerability, digital signature information system audit etc.
5. Clearing and settlement arrangement for electronic banking and electronic money transfer; linkages between i-banking and e-commerce.
6. Any other matter, which the Working Group may think as of relevance to Internet banking in India.

Keeping in view the terms of reference, the Group made a number of recommendations. A summary of these recommendations is given below.

1.7.2 Technology and Security Standards: [17]

The role of the network and database administrator is pivotal in securing the information system of any organization. Some of the important functions of the administrator via-a-vis system security are to ensure that only the latest versions of the licensed software with latest patches are installed in the system, proper user groups with access privileges are created and users are assigned to appropriate groups as per their business roles, a proper system of back up of data and software is in place and is strictly adhered to, business continuity plan is in place and frequently tested and there is a robust system of keeping log of all network activity and analyzing the same.

Organizations should make explicit security plan and document it. There should be a separate Security Officer I Group dealing exclusively with information systems security. The Information Technology Division will actually implement the computer systems while the Computer Security Officer will deal with its security. The Information Systems Auditor will audit the information systems.

Access Control:

Logical access controls should be implemented on data, systems, application software, utilities, telecommunication lines, libraries, system software, etc. Logical access control techniques may include user-ids, passwords, smart cards or other biometric technologies.

Firewalls:

At the minimum, banks should use the proxy server type of firewall so that there is no direct connection between the Internet and the bank's system. It facilitates a high level of control and in-depth monitoring using logging and auditing tools. For

sensitive systems, a Stateful inspection firewall is recommended which thoroughly inspects all packets of information, and past and present transactions are compared. These generally include a real-time security alert.

Isolation of Dial up Services:
All the systems supporting dial up services through modem on the same LAN as the application server should be isolated to prevent intrusions into the network as this may bypass the proxy server.

Security Infrastructure:
PKI is the most favored technology for secure Internet banking services. However, it is not yet commonly available. While PKI infrastructure is strongly recommended, during the transition period, until IDRBT or Government puts in place the PKI infrastructure, the following options are recommended:

- Usage of SSL, which ensures server authentication and the use of Client side certificates issued by the banks themselves using a Certificate Server.
- The use of at least 128-bit SSL for securing browser to web server communications and, in addition, encryption of sensitive data like passwords in transit within the enterprise itself.

Isolation of Application Servers:
It is also recommended that all unnecessary services on the application server such as ftp, telnet should be disabled. The application server should be isolated from the e-mail server.

Security Log (audit Trail):
All computer accesses, including messages received, should be logged. All computer access and security violations (suspected or attempted) should be reported and follow up action taken as the organization's escalation policy.

Penetration Testing:

The information security officer and the information system auditor should undertake periodic penetration tests of the system, which should include:

- Attempting to guess passwords using password – cracking tools.
- Search for back door traps in the programs.
- Attempt to overload the system using DdoS (Distributed Denial of Service) and DoS (Denial of Service) attacks.
- Check if commonly known holes in the software, especially the browser and the e-mail software exist.
- The penetration testing may also be carried out by engaging outside experts (often called "Ethical Hackers").

Physical Access Controls:

Though generally overlooked, physical access controls should be strictly enforced. The physical security should cover all the information systems and sites where they are housed both against internal and external threats.

Backup and Recovery:

The bank should have a proper infrastructure and schedules for backing up data. The backed-up data should be periodically tested to ensure recovery without Loss of transactions in a time frame as given out in the bank's security policy. Business continuity should be ensured by having disaster recovery sites, where backed-up data is stored. These facilities should also be tested periodically.

Monitoring against Threats:

The banks should acquire tools for monitoring systems and the networks against intrusions and attacks. These tools should be used regularly to avoid security breaches.

Education and Review:
The banks should review their security infrastructure and security policies regularly and optimize them in the light of their own experiences and changing technologies. They should educate on a continuous basis their security personnel and also the end users.

Log of Messages:
The banking applications run by the bank should have proper record keeping facilities for legal purposes. It may be necessary to keep all received and sent messages both in encrypted and decrypted form. (When stored in encrypted form, it should be possible to decrypt the information for legal purpose by obtaining keys with owners' consent.)

Certified Products:
The banks should use only those security solutions/products which are properly certified for security and for record keeping by independent agencies (such as IDRBT).

Maintenance of Infrastructure:
Security infrastructure should be properly tested before using the systems and applications for normal operations. The bank should upgrade the systems by installing patches released by developers to remove bugs and loopholes, and upgrade to newer versions which give better security and control.

Approval for I-banking:
All banks having operations in India and intending to offer Internet banking services to public must obtain an approval for the same from RBI. The application for approval should clearly cover the systems and products that the bank plans to use as well as the security plans and infrastructure. It should include sufficient details for RBI to evaluate security, reliability, availability, audit ability, recoverability, and other important aspects of the services. RBI may provide model documents for Security Policy, Security Architecture, and Operations Manual.

1.7.3 Legal Issues: [18]

The banks providing Internet banking service, at present are only accepting the request for opening of accounts. The accounts are opened only after proper physical introduction and verification. Considering the legal position prevalent, particularly of Section 131 of the Negotiable Instruments Act, 1881 and different case laws, the Group holds the view that there is an obligation on the banks not only to establish the identity but also to make enquiries about integrity and reputation of the prospective customer. The Group, therefore, endorses the present practice but has suggested that after coming in to force of the Information Technology Act, 2000 and digital certification machinery being in place, it may be possible for the banks to rely on digital signature of the introducer.

The present legal regime does not set out the parameters as to the extent to which a person can be bound in respect of an electronic instruction purported to have been issued by him. Generally authentication is achieved by security procedure, which involves methods and devices like user-id, password, personal identification number (PIN), code numbers and encryption etc., used to establish authenticity of an instruction. However, from a legal perspective a security procedure needs. to be recognized by law as a substitute for signature. In India, the Information Technology Act, 2000, in Section 3(2) provides for a particular technology (viz., the asymmetric crypto system and hash function) as a means of authenticating electronic record. This has raised the doubt whether the law would recognize the existing methods used by banks as valid methods of authentication. The Group holds the view that as in case of other countries, the law should be technology neutral.

In keeping with the view that law should be technology neutral, the Group has recommended that Section 3(2) of the Information Technology Act, 2000 needs to be amended to provide that in addition to the procedure prescribed there in or that

may be prescribed by the Central government, a security procedure mutually agreed to by the concerned parties should be recognized as a valid method of authentication of an electronic document / transaction during the transition period. Banks may be allowed to apply for a license to issue digital signature certificate under Section 21 of the Information Technology Act, 2000 and function as certifying authority for facilitating Internet banking. Reserve Bank of India may recommend to Central Government for notifying the business of certifying authority as an approved activity under clause (0) of Section 6(1) of the Banking Regulations Act, 1949.

Section 40A(3) of the Income Tax Act, 1961 recognizes only payments through a crossed cheque or crossed bank draft, where such payment exceeds Rs. 20,000/-, for the purpose of deductible expenses. Since the primary intention of the above provision, which is to prevent tax evasion by ensuring transfer of funds through identified accounts, is also satisfied in case of electronic transfer of funds between accounts, such transfers should also be recognized under the above provision. The Income Tax Act, 1961 should be amended suitably. Under the present regime there is an obligation on banks to maintain secrecy and confidentiality of customer's account. In the Internet banking scenario, the risk of banks not meeting the above obligation is high on account of several factors like customers not being careful about their passwords, PIN and other personal identification details and divulging the same to others, banks sites being hacked despite all precautions and information accessed by inadvertent finders.

Banks offering Internet banking are taking all reasonable security measures like SSL access, 128 bit encryption, firewalls and other net security devices, etc. The Group is of the view that despite all reasonable precautions, banks will be exposed to enhanced risk of liability to customers on account of breach of secrecy, denial of service etc., because of hacking / other technological failures. The banks should,

therefore, institute adequate risk control measures to manage such risk. In Internet banking scenario there is very little scope for the banks to act on stop - payment instructions from the customers. Hence, banks should clearly notify to the customers the timeframe and the circumstances in which any stop - payment instructions could be accepted.

The banks providing Internet banking service and customers availing of the same are currently entering into agreements defining respective rights and liabilities in respect of Internet banking transactions. A standard format / minimum consent requirement to be adopted by banks may be designed by the Indian Banks Association, which should capture all essential conditions to be fulfilled by the banks, the customers and relative rights and liabilities arising there from. This will help in standardizing documentation as also develop standard practice among bankers offering Internet banking facility.

The concern that Internet banking transactions may become a conduit for money laundering has been addressed by the Group. Such transactions are initiated and concluded between designated accounts. Further, the proposed Prevention of Money Laundering Bill 1999 imposes obligation on every banking company to maintain records of transactions for certain prescribed period. The Banking Companies (Period of Preservation of Records) Rules, 1985 also require banks to preserve certain records for a period ranging between 5 to 8 years. The Group is of the view that these legal provisions which are applicable to all banking transactions, whether Internet banking or traditional banking, will adequately take care of this concern and no specific measures for Internet banking is necessary.[19]

The Consumer Protection Act, 1986 defines the rights of consumers in India and is applicable to banking services as well. Currently, the rights and liabilities of customers availing of Internet banking services are being determined by bilateral

agreements between the banks and customers. It is open to debate whether any bilateral agreement defining customers rights and liabilities, which are adverse to consumers than what is enjoyed by them in the traditional banking scenario will be legally tenable. Considering the banking practice and rights enjoyed by customers in traditional banking, it appears the banks providing I-banking may not absolve themselves from liability to the customers on account of unauthorized transfer through hacking. Similar position may obtain in case of denial of service. Even though, The Information Technology Act, 2000 has provided for penalty for denial of access to a computer system (Section - 43) and hacking (Section - 66), the liability of banks in such situations is not clear. The Group was of the view that the banks providing Internet banking may assess the risk and insure themselves against such risks.

The Information Technology Act, 2000, in Section 72 has provided for penalty for breach of privacy and confidentiality. Further, Section 79 of the Act has also provided for exclusion of liability of a network service provider for data travelling through their network subject to certain conditions. Thus, the liability of banks for breach of privacy when data is travelling through network is not clear. This aspect needs detailed legal examination. The issue of ownership of transactional data stored in banks computer systems also needs further examination.[20]

1.7.4 Regulatory and Supervisory Issues:[21]

All banks, which propose to offer transactional services on the Internet, should obtain approval from RBI prior to commencing these services. Bank's application for such permission should indicate its business plan, analysis of cost and benefit; operational arrangements like technology adopted, business partners and third party service providers and systems and control procedures the bank proposes to adopt for managing risks, etc. The bank should also submit a security policy covering recommendations made in Chapter-6 of this report and a certificate from

an independent auditor that the minimum requirements prescribed there have been met. After the initial approval the banks will be obliged to inform RBI any material changes in the services / products offered by them.

RBI may require banks to periodically obtain certificates from specialist external auditors certifying their security control and procedures. The banks will report to RBI every breach or failure of security systems and procedure and the latter, at its discretion, may decide to commission special audit / inspection of such banks.

To a large extent the supervisory concerns on Internet banking are the same as those of electronic banking in general. The guidelines issued by RBI on "Risks and Controls in Computers and Telecommunications" will equally apply to Internet banking. The RBI as supervisor would cover the entire risks associated with electronic banking as a part of its regular inspections of banks and develop the requisite expertise for such inspections. Till such capability is built up, RBI may outsource this function to qualified EDP auditors.

Record maintenance and their availability for .inspection and audit is a major supervisory focus. RBI's guidelines on "Preservation and Record Maintenance" will need .to be updated to include risks heightened by banking on the net. The enhancements will include access to electronic record only by authorized officials, regular archiving of data, a sufficiently senior officer to be in charge of archived data with well defined responsibilities, use of proper software platform and tools to prevent unauthorized alteration of archived data, availability of data on - line, etc. If not available on - line, the system should be capable of making available the data for the same financial year within 24 hours and past data within a period of maximum 48 hours.

Banks should develop outsourcing guidelines to manage effectively, risks arising out of third party service providers such as risks of disruption in service, defective services and personnel of service providers gaining intimate knowledge of banks systems and misutilizing the same, etc. Alternatively, IBA or IDBRT may develop broad guidelines for use of the banking community.

With the increasing popularity of e-commerce, i.e., buying and selling over the Internet, it has become imperative to set up "Inter bank Payment Gateways" for settlement of such transactions. The Group have suggested a protocol for transactions between the customer, the bank and the portal and have recommended a framework for setting up of payment gateways. In their capacity as regulator of banks and payment systems of the country, the RBI should formulate norms for eligibility of an institution to set up a payment gateway and the eligible institution should seek RBI's approval for setting up the same.

Only institutions who are members of the cheque clearing system in the country may be permitted to participate in Inter - bank payment gateways for Internet payment. Each gateway must nominate a bank as the clearing bank to settle all transactions. Only direct debits and credits to accounts maintained with the participating banks by parties to an e-commerce transaction may be routed through a payment gateway. Payments effected using credit cards, payments arising out of cross border e-commerce transactions and all intra - bank payments (i.e., transactions involving only one bank) should be excluded for settlement through an inter - bank payment gateway.

Inter - bank payment gateways must have capabilities for both net and gross settlement. All settlement should be intra - day and as far as possible, in real time. It must be obligatory for payment gateways to maintain complete trace of any payment transaction covering such details like date and time of origin of transaction, payee, payer and a unique transaction reference number (TRN).

Connectivity between the gateway and the computer system of the member bank should be achieved using a leased line network (not through Internet) with appropriate data encryption standard. All transactions must be authenticated using user-id and password. Once, the regulatory framework is in place, the transactions should be digitally certified by any licensed certifying agency. SSL / 128 bit encryption must be used as minimum level of security. Adequate firewalls and related security measures must be taken to ensure privacy to the participating institutions in a payment gateway. Internationally accepted standards such as ISO 8583 must be used for transmitting payment and settlement messages over the network.

The RBI may have a panel of auditors who will be required to certify the security of the entire infrastructure both at the payment gateway end and the participating institutions end prior to making the facility available for customers use. The credit risk associated with each payment transaction will be on the payee bank. The legal basis for such transactions and settlement will be the bilateral contracts between the payee and payee's bank, the participating banks and service provider and the banks themselves. The rights and obligations of each party must be clearly stated in the mandate and should be valid in a court of law.

It will be necessary to make customers aware of risks inherent in doing business over the Internet. This requirement will be met by making mandatory disclosures of risks, responsibilities and liabilities to the customers through a disclosure template. The banks should also provide their latest published financial results over the net.

Hyperlinks from banks websites, often raise the issue of reputational risk. Such links should not mislead the customers in to believing that they sponsor any particular product or any business unrelated to banking. Hence, hyperlinks from a bank's websites should be confined to only those portals with which they have a

payment arrangement or sites of their subsidiaries or principals. Hyperlinks to banks website from different portals are normally meant to pass information pertaining to purchases made by banks' customers in the portal. Banks must follow the minimum recommended security precautions while dealing with such request, which includes customer authentication through user-id and password, independent confirmation of transaction by the customer and authorizing payment, use of SSL and 128 bit encryption for all communication both with the portal and customer browser terminal, etc.

On the question of additional capital charge on banks, which undertake Internet banking, the group held the view that standards have not yet been developed for measuring additional capital charge for operational risk. However, this requirement could be covered as the RBI moves towards risk based supervision.

The applicability of various existing laws and banking practices to E-banking is not tested and is still in the process of evolving, both in India and abroad. With rapid changes in technology and innovation in the field of E-banking, there is a need for constant review of different laws relating to banking and commerce. The Group, therefore, recommends that the Reserve Bank of India may constitute a multi disciplinary high level standing committee to review the legal and technological requirements of E-banking on continual basis and recommend appropriate measures as and when necessary.[22]

The regulatory and supervisory framework for E-banking is continuing to evolve and the regulatory authorities all over the world recognize the need for cooperative approach in this area. The Basle Committee for Banking Supervision (BCBS) has constituted an Electronic Banking Group (EBG) to develop guiding principles for the prudent risk management of E-banking activities. This Working Group, therefore, recommends that the Reserve Bank of India should maintain close contact

with regulating / supervisory authorities of different countries as well as with the Electronic Banking Group of BCBS and review its regulatory framework in keeping with developments elsewhere in the world.

The Group submitted its report in June 2001 and the Reserve Bank while accepting the recommendations of the Working Group, issued guidelines on "Internet Banking in India" for implementation by banks. It also stated that the earlier guidelines issued by the Reserve Bank on "Risks and Controls in Computers and Telecommunications" (1998) would equally apply to Internet banking as well. [23]

1.8 E-banking Challenges and Concerns: [24]

E-banking is based on technology that by its very nature is designed to expand the "virtual" geographic reach of banks and customers without necessarily requiring a similar "physical" expansion. Such market expansion can extend beyond national borders which significantly increase cross – border cooperation challenges for bank supervisors due to:

- The potential ease and speed with which banks located anywhere in the world can conduct activities with customers over interconnected electronic networks 4 into countries where a bank is not licensed or supervised.
- The potential ability of a bank or non – bank to use the Internet to cross borders and to seamlessly link banking activities that have typically been subject to supervision with non – banking activities that might be unsupervised by any financial market authority.
- The practical difficulties faced by national authorities wishing to monitor or control local access to E-banking sites originating in other jurisdictions without the cooperation of home country authorities.

Banking organizations have been delivering services to consumers and businesses remotely for years. Electronic funds transfer, including small payments and corporate cash management systems, as well as publicly accessible machines for currency withdrawal and retail account management are global fixtures. However, delivering financial services over public networks such as the Internet is bringing about a fundamental shift in the financial services industry.

The changes created, and some of the technical characteristics of internet technology raise new concerns for both bankers and supervisors. Banking organizations are focusing increasingly on their E-banking activities and are globally expanding Internet banking activities, exploring the use of wireless networks and venturing into some new areas of electronic commerce.

Banks offer E-banking services to defend or expand market share or as a cost saving strategy to reduce paperwork and personnel. The Internet also provides banks with substantial opportunity to extend their customer reach beyond existing boundaries. However, the nature of the open network and the evolution of electronic commerce expose banks to significant competition from banking and non - banking firms. In addition, electronic delivery channels operate in an uncertain legal and regulatory environment that differs by jurisdiction. [25]

All these factors present new challenges for financial institutions in managing security, integrity and availability of services provided while remaining sufficiently profitable. Following are the emerging trends and issues that could impact bank risk profiles:

1. A significant increase in competition in the electronic financial services industry as both, banking and non - banking firms rapidly introduce new financial products and services.

2. Rapid technological improvements in telecommunications and computer hardware and software enabling greater speed in transactions processing.
3. Bank management and staff often lack expertise in technology and E-banking risk issues.
4. Greater reliance on outsourcing to third party service providers, and a proliferation of new alliances and joint ventures with non - financial firms.
5. Greater demand for global infrastructures for technology that are scalable, flexible and interoperable, both within and across enterprises and that can ensure the security, integrity and availability of information and services.
6. Increased potential for fraud, due to the absence of standard business practices for customer verification and authentication on open networks like the Internet.
7. Legal and regulatory ambiguity and uncertainty with respect to the application and jurisdiction of current laws and regulations to evolving E-banking activities.
8. The collection, storage and frequent sharing of significant quantities of customer data can lead to customer privacy issues that potentially create prudential risks for banks (e.g. legal and reputational).
9. Questions regarding the effectiveness and efficiency of online disclosures. Lengthy or complicated online disclosures may cause customers to simply "click through" or even quit a web site; moreover, extensive disclosure reduces the speed at which web sites and pages can be downloaded.

Banks and bank supervisors generally agree that the supervisory principles that apply to traditional banking are applicable to E-banking. However, the combination of rapid changes in technology and the degree of bank dependence on technology vendors and service providers modify and sometimes magnify traditional risks. Hence, there is a need for additional supervisory guidance in selected areas to enhance the overall risk management framework for E-banking activities.

These developments in E-banking to date suggest that:

- ❖ The desire to benefit from the advantages of e-commerce in financial services has become widespread. The financial services industry is increasingly focused on providing technology based financial services solutions directly to customers in order to help build and retain customer bases.
- ❖ Speed to market has become a critical factor for success in E-banking. To reduce time to market, banking institutions are allying with non-banking firms to provide total financial services solutions.
- ❖ The current trends in the formation of strategic alliances and technology outsourcing will grow.

These developments present challenges for both banks and bank supervisors. Bank management needs to re-evaluate the robustness of traditional risk management practices in light of the new risks posed by E-banking activities. Also, bank supervisors need to take a balanced approach to the introduction of new regulation and supervisory policy on E-banking, so as to .ensure safe and sound operations of banks while at the same time not stifling innovation and the competitiveness of the banks relative to non-banks.

1.9 E-banking: Risks and Their Management: [26]

E-banking using the Internet as an added delivery channel may shift bank risk profiles to some degree and create new risk control challenges for banks. Accordingly, bank supervisors need to consider the implications of a bank's use of the E-banking delivery channel on its strategic risk, operational risk, reputational risk, legal risk, credit risk, liquidity risk, market risk and foreign exchange risk.

1.9.1 Strategic and Business Risk: [27]

Strategic risk is one of the most significant risks that E-banking activities present for banking organizations. Strategic risk differs from' other risk categories in that it is more general and broad in nature. Strategic decisions to be taken by a bank's Board of Directors and executive management will have implications for all other risk categories.

Given growing customer acceptance and demand for E-banking, as well as the potential efficiencies afforded, most banks will need to develop a strategy to use the Internet delivery channel to provide informational content and/or transactional service to customers. The rapid changes in technology, the pace of competition with other banks and non bank competitors and the nature of that strategy could expose banks to substantial risk if the planning and implementation of the strategy is flawed or otherwise not well thought through.

Some of the strategic risks involved with E-banking are directly linked with timing issues. There can be significant strategic risk associated with a management decision to be a technology pioneer, particularly if the institution becomes burdened with systems made redundant by rapid technological changes. Likewise, an overly cautious technology follower may find itself unable to adequately position itself in a saturated market or a market that is consolidating rapidly.

Prior to the Internet, banking institutions used proprietary networks within their consolidated enterprise and connected in limited ways to other banks. These proprietary networks helped provide a strategic defence against new entrants and provided individual franchise protection. However, the Internet as an open network with open access allows both banks and non banks freedom to create and leverage existing business without the need for expanded physical presence. Consequently, competition within the financial services industry has been significantly increased and is likely to increase further.

Most bankers believe that the E-banking delivery channel will enable them to reduce operational expenses. However, many bank customers wish to maintain a traditional banking relationship, which makes it difficult for banks to abandon the existing physical infrastructure. This means that banks will at least for the foreseeable future need to run multiple delivery channels for sometime and E-banking will be a net additional expense. Thus, operational expense savings may occur over the long run only.

The challenge the banking industry faces in maintaining market share is complicated by the entry of new firms that ate providing individual financial services via the Internet to existing bank customers. The emergence of aggregation and screen scraping technologies poses both strategic opportunities and threats to banks. Depending on the evolving relationship between the aggregator, the banks affected and the consumer, banks may get further disintermediated as aggregators potentially disrupt the traditional relationship between the customer and the bank and "limit" the direct access that banks will have on - line to retail customers. In addition, aggressive aggregation by both banks and non-banks may lead to greater commoditization of banking products and services, thereby reducing bank profit margins and adding new security and legal risks.

In essence, bank management needs to carefully consider how its Internet strategy will help maintain the competitiveness and profitability of the institution yet not lead to unwarranted increases in its risk profile. Supervisors should expect banking institutions to carefully assess the pros and cons associated with their strategic options.

1.9.2 Operational Risk: [28]

Because of the reliance on technology for all facets of E-banking, operational risk is one of the more significant risks. To limit operational risk, banking organizations may want to consider implementing an integrated enterprise - wide architecture and technology infrastructure that can facilitate inter operability, ensure the security, integrity and availability of data and support the management of relationships with third - party service providers. Further, as technology is also dramatically changing business models and operating processes, banks need to ensure that they have appropriate control procedures (including change control) and audit processes.

Technology Infrastructure:

E-banking has brought the issue of technological systems and applications integration to the forefront. Many large banks are now faced with the task of integrating systems for E-banking activities with their existing legacy systems and with the systems of multiple service providers and partners. These banks are exposed to significant operational risks from errors in transaction processing if the systems for E-banking are not properly integrated.

Accordingly, many large banks are making significant investments in technology infrastructure in order to create improved internal controls and enhanced risk management oversight processes. The banks are also hoping to improve flexibility, scalability and interoperability of their systems and operations both within their enterprises and across outside service providers.

While these general developments by large banks are positive, in general the banking industry has much further to go towards improving its systems and risk management infrastructure to effectively support E-banking. Small to medium-sized banking organizations are particularly challenged because of budget

restrictions for acquiring hardware and software, as well as attracting and keeping technical staff. Many of these banks rely significantly on third party service providers to manage the necessary technological infrastructure to support the bank's E-banking operations. In this situation, the bank still retains ultimate responsibility for ensuring that these operations are well controlled and managed, and the bank supervisor will wish to assess the ongoing ability of bank management to do so adequately.

Security: [29]
The majority of bankers surveyed by EBG members identified security risk as a primary concern relating to E-banking. External threats such as "hacking", "sniffing", "spoofing" and "denial of service" attacks expose banks to new security risks. Open electronic delivery channels create new security issues for banks with respect to confidentiality and integrity of information, non-repudiation of transactions, authentication of users and access control.

Most banks appear to be sensitive to external security threats. Among the issues identified for immediate attention is the development of more robust tools to verify the identity and authenticity of larger value transaction requests. In addition, the banking industry needs to continue to work towards international best practices for encryption requirements, including the legality of electronic signature and records. Moreover, since many banks' internal networks rely on security technology similar to that used to manage their external systems, it is important that bankers also be sensitive to managing the security risk arising from their internal networks. If not managed properly, internal security exposures can also compromise the integrity and confidentiality of bank records and customer data.

Poor security may create reputational or legal risks for banks, as they may be deemed to have provided inappropriate protection for customers' personal data, with consequential legal and / or reputational damage.

At the international level, bank supervisors should encourage the development of a comprehensive approach to managing risk associated with both internal and external security exposures. Given the continuing evolution of industry standards, security risk management may be an area where bank supervisors can work collaboratively with the industry to promote the development of sound practices.

Data Integrity: [30]

Data integrity is an important component of system security. Banking organizations must improve interoperability within and across enterprises to effectively manage relationships with customers, other banks and external service providers. Until industry standards are identified for electronic data management, banking organizations will continue to be challenged to establish effective control processes to ensure the accuracy and integrity of data being transmitted and received. The processes should include, at a minimum, sound policies and practices related to project management, system development life cycle, change control and quality assurance. Bank supervisors should also encourage banks to review the integrity of the data used by their risk management systems.

Given the lower cost and ubiquitous nature of the Internet, organizations are increasingly using TCP / IP as a standard communications protocol to achieve this. While there are significant benefits of communicating via TCP / IP, organizations must ensure that data transmitted between bank legacy systems and systems of other parties are translated and integrated accurately. Moreover, while the introduction of middleware and languages such as XML are helping to facilitate this effort, the development of industry standards to support these new technologies is still in its very early stages.

System Availability: [31]

In addition to ensuring a secure internal network for their E-banking activities, effective capacity planning is critical to ensuring the ongoing availability of E-banking products and services. Transaction volumes may become increasingly volatile due to price sensitivities and greater automation. Also, competitive pressures and increased reliance on having services available 24 hours a day and 7 days a week (24 x 7) have raised customer expectations considerably and in turn reduced the tolerance for error. To compete effectively and avoid potentially significant reputation risk that could arise from systems outages, banks offering E-banking services must deliver the right mix of products and services securely, accurately and consistently. These factors underscore the importance of effective business continuity, recovery and incident response plans. Moreover, trends in outsourcing make it necessary for bankers to ensure that similar plans are in place at their external service providers and are periodically tested for effectiveness.

Denials of service attacks can also reduce or eliminate a bank's ability to serve its customers while under attack. These attacks have become increasingly common against high profile e-commerce providers. An added challenge is posed by banks inability to control the availability of the Internet network itself. Thus, a bank needs to consider, as part of its contingency plans, alternative means to deliver service in the event of a major disruption to the Internet network.

Internal Controls / Audit: [32]

The ability to detect and correct errors is a critical internal control component of any banking operation. Moreover, banking organizations must have sufficient controls in place to prevent fraud from both internal and external sources and safeguard the bank's information and assets.

Much of the efficiency and cost reduction in E-banking services stem from banks ability to implement "straight - through processing". While the benefits of straight - through processing are many, the reality is that E-banking modifies how internal controls, proper segregation of duties and clear audit trails are applied over broad access channels. The challenges presented by these changes are compounded by a critical shortage of skills and expertise in the industry in. both the operations and audit areas. Going forward, banks will be increasingly challenged to ensure that highly automated environments provide effective control and that the controls can be independently audited.

Outsourcing: [33]

Perhaps more than any other industry development relating to E-banking, banks' increased reliance on outsourcing is having a significant impact on the risk profiles of all banking organizations - both large and small. Large banks are outsourcing many activities as they are increasingly focusing on their core businesses and partnering with other organizations for solutions outside of their core competencies. Small banks usually must outsource because they often lack the necessary technical expertise and resources to build an E-banking delivery channel on their own. Additionally, a decline in the cost of "turnkey" solutions has made it more affordable for small banks to purchase E-banking applications from vendors. These developments are positive in that they increase efficiency, they allow smaller institutions to compete more effectively and they promote the introduction of "state of the art" applications within the industry. However, they can also substantially add to banks challenges in managing operational risk.

Preliminary indications from surveys tend to indicate that financial institutions rely upon a relatively small number of third - party providers. This seems to be especially the case for small to medium-sized institutions. In some cases, these third parties happen to be new firms with a relatively short track record. This apparent

reliance on a concentrated number of third parties, which the EBG will investigate further, could have systemic implications if a major problem would arise with one of these service providers.

To properly manage the risks associated with outsourcing, banks must conduct appropriate due diligence and monitoring of the ongoing viability of third party service providers. The adequacy of terms under contract and service level agreements must also be carefully reviewed for legal risk. Operations processing and the management of security, integrity and availability risks are also more complicated. Furthermore, many technology providers and partners are newly established and may lack knowledge of the controls required within a banking environment. Minor disruptions on the part of third party service providers can expose banking organizations to potential financial loss and substantial legal and reputation risk. Complexity is also added by multiple vendor / service provider relationships that often support E-banking operations. Although to date such disruptions seem to have been controlled, in the future their potential impact could be quite considerable and raises significant concerns for supervisors and industry participants.

Outsourcing can lead to additional privacy related risk exposures. Banks may not always be aware of the exact collection and usage of customer data by vendors and other third parties, and / or may not be adequately managing such activities. Moreover, the legal rights and responsibilities of service providers and vendors may not always be clear. Banks should be encouraged to address privacy issues in their contractual and ongoing relations with vendors.

Various bank supervisors around the world have developed specific guidance related to technology outsourcing. The EBG plans to conduct a review of such guidance and to explore ways to coordinate the development of sound practices in this area for both the banking industry and its supervisors.

1.9.3 Reputational Risk: [34]

A bank's reputation can be impacted by any adverse development that precludes the availability of their E-banking delivery channel. Banks have long based their business on a reputation of trust. The ability to provide a trusted network to support E-banking is critical, and a bank's reputation can be damaged by Internet banking services that are poorly executed or otherwise alienate customers and the public.

A bank's reputation can suffer if it fails to deliver secure, accurate and timely E-banking services on a consistent basis. A bank's reputation can also be adversely impacted if it fails to respond to inquiries posted via e-mail, does not provide proper disclosure, or violates customer privacy. Hypertext links from a bank to third party web sites or outsourced service providers may cause customer confusion about the provider of specific products and services offered, and whether they are insured or uninsured. Customers can also be confused about whether the links from the bank reflect an implied endorsement of the third party's products or services and may well look to the bank for recourse if problems are encountered.

Further, major security breaches in a bank or a non - bank competitor's web site could undermine overall consumer or market confidence in banks ability to appropriately manage Internet-based transactions. Any problems that a bank might experience with regard to data and privacy protection could threaten the reputation of that bank as well as the reputation of any other banks perceived to be involved in similar activities.

To protect against adverse situations that may cause damage to their reputation, banking organizations should develop and monitor performance standards for their E-banking activities. Regular review and testing of business continuity, recovery and incident response plans, and communications strategies are also critical to protecting banks reputations.

1.9.4 Legal Risk: [35]

Legal risk arising from E-banking activities represents another area of increased concern. Currently, supervisors in every jurisdiction are examining how existing legal and regulatory frameworks originally designed to address issues affecting the "physical" world of banking interact with the developing E-banking delivery channel as well as examining potential ambiguities.

A bank that develops relationships via the Internet with customers in other jurisdictions may be unfamiliar with the banking and customer protection laws and regulations specific to those countries and may consequently incur heightened legal risks. Even banks that do not intend to solicit business from consumers in foreign jurisdictions may find that their offerings on-line are considered solicitations in. some countries. For example, if a bank makes its web site available in another language, regulators in any country where that language is spoken may determine that the bank is marketing services to its citizens and may find that the bank is therefore subject to its local laws and regulations.

Unauthorized use or misuse of data collected over the Internet is another potential Source of legal risk. Unauthorized individuals can attack and / or try to infiltrate the "data warehouses" maintained about consumers by both banks and third party vendors. For example, hackers or others might break into banks' or vendors' databases or build their own databases and use the consumers' information to perpetrate fraud. Authorized staff may also deliberately misuse data. Surveys of banks and third party vendors conducted by the EBG have showed that such attacks on "data warehouses" have already occurred, although the impact of these attacks has been minimal to date.

The enforceability of certain emerging areas of law is also uncertain. Laws related to the enforceability of electronic contracts and digital signatures are still under

development and vary from jurisdiction to jurisdiction. Effective "know your customer" (KYC) practices are also becoming more critical to bankers in their attempts to prevent fraud.

1.9.5 Other Traditional Banking Risks: [36]

The E-banking delivery channel also has implications for other traditional banking risks such as credit risk, liquidity risk, interest rate risk, and market risks. The impact of the introduction of E-banking does not necessarily result in an increase or decrease in the risk profile of the institution, but risks can be shifted, sometimes in complex ways.

Credit Risk:

The credit risk of a banking institution can be affected by E-banking activities in a number of ways. The use of the Internet delivery channel may allow banks, especially small institutions, to expand very rapidly, which could lead to heightened asset quality and internal control risks. The use of the Internet also allows banks to expand their geographic reach out of their traditional area, which increases the challenge of understanding local market dynamics and risks, verifying collateral and perfecting security liens with out of area borrowers. In addition, the Internet also makes it more difficult to authenticate the identity and creditworthiness of a potential customer, which are essential elements to sound credit decisions. Further, there has been a tendency for some Internet only banks to pay higher rates on deposits opened over the Internet, which could lead to a higher level of sub-prime credits at these institutions in order to support these higher deposit rates. These factors underscore the importance of sound credit under writing policies, credit monitoring and administration practices regardless of which product delivery channel is used.

Liquidity Risk:

The speed with which information and misinformation moves over the Internet can have implications for the liquidity risk profile of a bank. Adverse information about a bank, whether it is true or not, can be easily disseminated over the internet through bulletin boards and news groups. This could cause depositors to withdraw their funds in mass at any time of the day, any day of the week. Also, internet banking can increase deposit volatility to the extent that new customers brought in through this channel maintain accounts solely on the basis of interest rate or terms. Accordingly, increased monitoring of liquidity and changes in deposits and loans may be warranted depending on the volume of activity created through E-banking.

Market Risk:

The impact of recent growth in securities issuance and trading over the internet on banks market risk profiles is complex. From a market standpoint, the increased volume of securities, which are traded over the Internet, can on the one hand lead to increased volatility, but, on the other hand, it can lead to increased liquidity. From an individual bank's standpoint, banks may be exposed to increased market risk if they create or expand deposit brokering, loan sales, or securitization programme as a result of internet banking activities. As with liquidity risk, the effects of increased E-banking activities on market volatility need to be monitored by banks and supervisors.

Foreign Exchange Risk: [37]

A bank may be exposed to foreign exchange risk if it accepts deposits from foreign customers or create accounts denominated in currencies other than their local currency. Since the Internet allows banks the opportunity to expand their geographic range, even internationally, some banks may take on greater foreign exchange risk through E-banking activities than they have through their traditional delivery channels. Also, foreign exchange risk can be intensified by political, social

or economic developments, which a bank inexperienced in cross - border banking may not appreciate fully. Supervisors should ensure that a bank initiating cross-border E-banking activities through the Internet has the appropriate risk management systems and expertise to manage these risks properly.

As the preceding discussion indicates, the basic types of risks associated with E-banking are not new. However, the specific ways in which these risks arise, as well as the potential magnitude and speed of impact on banks, may be new for bank management and supervisors alike. In addition, while assessing risk should already be dynamic, the rapid pace of technological innovation supporting E-banking, the increased degree of systems outsourcing and the reliance of some products / services on the use of open networks such as the Internet, intensifies the need for a rigorous and ongoing risk management process.

Bank supervisors should expect their banks to have comprehensive risk management processes in place that include the three basic elements of assessing risks, controlling risk exposure, and monitoring risks associated with E-banking. This comprehensive risk management framework should be integrated into the bank's overall risk management framework. [38]

It is also essential that this risk management process is supported by appropriate oversight by the board of directors and senior management and is carried out by staff with the necessary knowledge and skills to deal with the technical complexities of new E-banking developments.

Similarly, bank supervisors must recognize their own critical need for supervisory staff with appropriate technology knowledge and skills to ensure that they understand the risks and challenges arising from the development of the E-banking delivery channel. Enhanced technical training of existing supervisory staff,

complemented by appropriate recruitment of outside expertise, should be a high priority in order to ensure that the supervisor keeps abreast of increasingly complex technology and market developments.